UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/815,396	03/31/2004	Christopher J. Lord	110466-152116	7579

31817 7590 02/08/2008
SCHWABE, WILLIAMSON & WYATT, P.C.
PACWEST CENTER, SUITE 1900
1211 S.W. FIFTH AVE.
PORTLAND, OR 97204

EXAMINER	
ZHANG, SHIRLEY X	

ART UNIT	PAPER NUMBER
4121	

MAIL DATE	DELIVERY MODE
02/08/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/815,396	**Applicant(s)** LORD ET AL.	
	Examiner SHIRLEY X. ZHANG	**Art Unit** 4121	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9 and 11-37* is/are rejected.

7)☒ Claim(s) *10* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03/31/2004* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

This non-final office action is responsive to the U.S. patent application filed March 31, 2004.

Claims 1-37 are pending;

Claims 1-9, 11-27 are rejected;

Claim 10 is objected to.

Claim Rejections - 35 USC § 112

1. Claim 23 recited the limitation "the second device". There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 27, 32 and 36 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 27 and 32 recite "An article comprising a machine-accessible media" which does not fall into any statutory categories of patentable subject matter.

Claims 28-31 and 32-35 depend on claims 27 and 32, respectively, therefore inherit the 35 U.S.C. 101 issues of the independent claims.

Claim 36 recites "machine accessible information" which does not fall into any statutory categories of patentable subject matter.

Claim 37 depends on claims 36, therefore inherits the 35 U.S.C. 101 issue of the independent claim.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

3. **Claims 1-9, 11, 27-31, 36 and 37** are rejected under 35 U.S.C. 103(a) as being unpatentable over the U.S. patent application publication no. 2003/0217136 to Cho et al. (hereinafter "**Cho**"), in view of U.S. patent application publication no. 2003/0217165 to Buch (hereinafter "**Buch**"), U.S. patent publication no. 2005/0111382 to Le et al. (hereinafter "**Le**"), and the article "UPnP™ Security Ceremonies Design Document 1.0" authored by Ellison and published by the UPnP Forum (hereinafter "**Ellison**").

Regarding claims 1, 27 and 36, Cho teaches a method, an article comprising a machine-accessible media having associated data, and machine-accessible information, for an intermediary selectively coupling an external network and an internal network to dynamically generate filter rules to facilitate establishing an end to end session connection between a first device on the internal network and a second device of the external network (Fig. 1 and [0026] disclose the proxy server 130 that is equivalent to the intermediary recited in the claim), the method comprising:

receiving a session establishment request by the second device on the external network to establish a communication session with the first device on the internal network (Fig.7 and [0026] disclose that the UPnP proxy server includes an agent 131 for receiving a command from the wired and wireless clients 100 or 110 on the Internet);

forwarding the session establishment request to the first device (Fig.7 and [0026] disclose that the UPnP proxy server also includes a bridge for sending control messages to the UPnP devices in the home network);

monitoring the internal network for an approval or disapproval acknowledgement by the first device for the session establishment request (Fig.2, Fig.7 and [0026] disclose that the bridge receive event messages from the UPnP devices, where the event messages include responses to the previously sent control messages); and

Cho does not disclose that the session to be established is a secure session.

However, in the same field of endeavor, Buch teaches a way of performing end-to-end user authentication to establish secure sessions using the SIP Invite request and responses, as disclosed in its Abstract.

It would have been obviousness for one of ordinary skill to combine Cho and Buch to have a system that establishes secure sessions between two network terminal devices via by using end-to-end authentication. One would have been motivated to combine as such by Ellison's teaching of the need for a security model which need was recognized by the UPnP Forum at the time of the invention (see Ellison, page 3, section 1 “Background” and section 2 “Security Model”), and that Buch’s teaching of an end-to-end authentication mechanism provides a solution to the problem.

Furthermore, Cho does not disclose that if an approval acknowledgement is monitored, then configuring a first filter rule of the intermediary to allow communication between the first and second devices through the intermediary.

However, in the same field of endeavor, Le discloses using firewall pinholes to dynamically filter network packets (see [0002]), where the firewall is an intermediary whose filtering rules are dynamically configured and applied based on the newly established or deleted network address bindings for authorized communications (see [0137] and [0138]).

It would have been obviousness for one of ordinary skill to combine Cho and Le such that a firewall is employed to allow communications between authenticated sessions only by using dynamically configured filtering rules. One would have been motivated to combine as such by Le's teaching of using an Internet firewall to secure an internal network from the Internet to the extent that it blocks unsolicited traffic from the outside.

Regarding claims 2 and 28, the combination of Cho, Buch, Ellison and Le teaches the method of claim 1, and the article of claim 27, respectively.

Cho further teaches that the method comprises:

determining a presence advertisement for the first device has been received before forwarding the secure session establishment request to the first device (Cho, Fig. 2, Fig. 7 and [0039] disclose that the device management module 21 is adapted to receive advertisement messages periodically sent from the UPnP devices in the home network, manage a device list on the basis of the received advertisement messages and, when a new UPnP device is additionally provided in the home network, receive a device description from the new UPnP device).

Regarding claim 3, the combination of Cho, Buch, Ellison and Le teaches the method of claim 2.

Cho further teaches that the presence advertisement is delivered in accordance with the UPnP Simple Service Discovery Protocol (SSDP) (Cho, [0008] discloses using SSDP, a protocol proposed to be used in UPnP network for presence advertisement).

Regarding claim 4, the combination of Cho, Buch, Ellison and Le teaches the method of claim 1. Cho further teaches that the method comprises:

receiving network traffic from the second device corresponding to the second device requesting a UPnP Device Description Document from the first device (Cho, Fig. 7 and [0071] disclose that upon receiving a service description request message from the stub 102 (step 717), the agent 131 sends the received message to the bridge 132 (step 718), which then transfers it to the specific UPnP device (step 719)).

Regarding claims 5, 29 and 37, the combination of Cho, Buch, Ellison and Le teaches the method of claim 1, the article of claim 27 and the propagated signal of claim 36, respectively.

Cho does not teach but Le teaches:

receiving a service request from the second device for the first device, the service request having an associated communication port for performing the service (Cho, [0097] discloses that the UE sends a SIP Invite to its CPS, specifying the IP address IP1, as well as the port number where it expects the media stream in the SDP (Session Description Protocol) field);

determining the service request identifies a service advertised by the first device in a device description document; and configuring a second filter rule to allow communication between the first device and the second device using the associated communication port (Cho, [0149] discloses that a communication security can be achieved by analyzing the SIP signaling and the data exchanged between the communicating nodes, more particularly by analyzing the indicated IP addresses (and optionally port numbers) which serve as the "dynamic rules" for the firewall, such disclosure implies that the firewall is configured with filter rules that use the associated communication ports).

Examiner provides the same rationale as provided in the rejection of claim 1 for the combination of Cho and Le.

Regarding claims 6 and 30, the combination of Cho, Buch, Ellison and Le teaches the method of claim 1 and the article of claim 27 respectively.

Cho further teaches that the method comprises:

providing the second device with an indicia for use by the second device in establishing a communication link to the first device (Fig.7 and [0071] disclose that the specific UPnP device sends the service description to the bridge 132 (720), which then transfers it to the agent 131 (721), where the service description is equivalent to the indicia recited in the claim).

Regarding claim 7, the combination of Cho, Buch, Ellison and Le teaches the method of claim 1.

Cho further teaches that the indicia is a selected one of a globally routable Internet Protocol (IP) address, or an internal network address non-routable on the external network ([0008] discloses a method that is adapted to control UPnP devices with private Internet protocol (IP) addresses in a home network over the Internet by providing on the Internet a UPnP directory server that translates uniform resource locator (URL) information in device descriptions of the UPnP devices by way of a network address translation (NAT) technology and provides the translated information to a client on an external Internet network; as NAT translates between public and private IP addresses, IPv6 and IPv4 address, or private IP addresses of different subnets, the use of NAT in Le implies that the address returned to the UE in the external network is either a public IP address, or a private IP address).

Regarding claim 8, the combination of Cho, Buch, Ellison and Le teaches the method of claim 1.

Cho does not teach but Le teaches that communication within the internal network is in accord with an IPv6 compatible Internet Protocol (IP) (Le, [0014] discloses that the architecture as illustrated in FIG. 1 has been recently adopted in 3GPP for the interworking of IPv6 and IPv4 domains; In 3GPP, it is inherent that the internal network uses IPv6).

Examiner provides the same rationale as provided in the rejection of claim 1 for the combination of Cho and Le.

Regarding claims 9 and 31, the combination of Cho, Buch, Ellison and Le teaches the method of claim 1 and the article of claim 27, respectively.

Cho does not teach but Ellison further teaches that the method comprises: retrieving an Access Control List (ACL) from the first device, the ACL including an identification of devices authorized to establish communication sessions; and determining based at least in part on the ACL the second device is authorized to establish the secure communication session with the first device before forwarding the secure session establishment request to the first device (Ellison, page 14, section “ACl editing” discloses that SOAP security is accomplished by an ACL in each secured device, each of the entries of grants some set of permissions on a device).

It would have been obvious for one of ordinary skill in the art to modify Cho with Ellison’s teaching so that Cho's UPnP Proxy maintains the ACL for each UPnP devices. One would have been motivated to combine as such by the need for security control in UPnP networks, as suggested by Ellison in page 3, section "Security Model".

Regarding claim 11, the combination of Cho, Buch, Ellison and Le teaches the method of claim 1.

Cho does not teach but Buch teaches establishing the end to end secure session connection between the first device on the internal network and the second device of the external network in a single end to end secure session connection between said first and second devices (Buch, Abstract discloses that the invention is related to an end-to-end authentication capability based on public-key certificates).

Examiner provides the same rationale as provided in the rejection of claim 1 for the combination of Cho and Buch.

4. **Claims 12, 15-20, 22 and 32-34** are rejected under 35 U.S.C. 103(a) as being unpatentable over the U.S. patent application publication no. 2003/0217136 to Cho et al. (hereinafter "**Cho**"), in view of U.S. patent application publication no. 2003/0217165 to Buch (hereinafter "**Buch**"), IETF draft "Simple Service Discovery Protocol/1.0" (hereinafter "**IETF-Draft-SSDP**"), and the article "UPnP™ Security Ceremonies Design Document For UPnP Device Architecture 1.0" authored by Ellison and published by the UPnP Forum (hereinafter "**Ellison**").

Regarding claims 12 and 32, Cho teaches a method and an article comprising a machine-accessible media having associated data for communicating with a device by way of an intermediary selectively coupling an external network and an internal network (Cho, Fig. 1 and

[0026] disclose the proxy server 130 that is equivalent to the intermediary recited in the claim), comprising:

receiving a presence advertisement for the device (Cho, Fig. 2, Fi.g7 and [0039] disclose that the the device management module 21 is adapted to receive advertisement messages periodically sent from the UPnP devices in the home network, manage a device list on the basis of the received advertisement messages and, when a new UPnP device is additionally provided in the home network, receive a device description from the new UPnP device);

storing a network address associated with the first device (Cho, [0015] discloses a method of allowing the UPnP proxy server to discover the UPnP devices in the home network, acquire information of the UPnP devices, create a device list on the basis of the acquired information; Cho, [0008] further discloses that a UPnP SSDP protocol is used, as SSDP was proposed by Microsoft as the protocol of choice for device discovery, see “IETF-Draft-SSCP-01”; furthermore, the SSDP draft discloses in section 5.2.1.1 an example of the presence announcement message, which includes a network address associated with the UPnP device; therefore, it can be implied that the UPnP proxy server stores a network address of the device in the device list).

determining services offered by the device (IETF-Draft-SSCP, section 5.2.1.1 discloses that the presence announcement messages contains a value “NT” which indicates the type of service offered by the device); and

while on the external network, issuing a communication initiation request to the device via the intermediary (Cho, Fig.7 disclose that the UPnP client sends commands to the UPnP device via the UPnP Proxy).

Cho does not teach that the request for the initiation of a secure communication session. However, , in the same field of endeavor, Buch teaches a way of performing end-to-end user authentication to establish secure sessions using the SIP Invite request and responses, as disclosed in its Abstract.

It would have been obviousness for one of ordinary skill to combine Cho and Buch to have a system that establish secure sessions between two network terminal devices via by using end-to-end authentication. One would have been motivated to combine as such by Ellison's teaching of the need for a security model which need was recognized by the UPnP Forum at the time of the invention (see Ellison, page 3, section 1 “Background” and section 2 “Security Model”), and that Buch’s teaching of an end-to-end authentication mechanism provides a solution to the problem.

Regarding claims 15 and 33, the combination of Cho, IETF-Draft-SSDP, Buch and Ellison teaches the method of claim 12 and the article of claim 32, respectively.

Cho further teaches that the presence advertisement is received while on the internal network (Cho, [0026] discloses that the bridge 132 in the UPnP proxy server receives the presence advertisement on the internal network).

Regarding claims 16 and 34, the combination of Cho, IETF-Draft-SSDP, Buch and Ellison teaches the method of claim 12 and the article of claim 32, respectively.

Cho further teaches that while on the internal network, the method comprises requesting a description of services offered by the device (Cho, Fig. 7 discloses in step 718 that the UPnP Proxy server requests a description of services offered by the device from the bridge interfacing to the internal network).

Regarding claim 17, the combination of Cho, IETF-Draft-SSDP, Buch and Ellison teaches the method of claim 16. Cho further discloses that the description of services is requested from the intermediary (Cho, Fig.17 discloses in steps 717 and 723 that the UPnP client requests the description of services from the UPnP proxy server, which is an intermediary).

Regarding claims 18 and 35, the combination of Cho, IETF-Draft-SSDP, Buch and Ellison teaches the method of claim 12 and the article of claim 32, respectively.

Cho further teaches that while on the external network, the method further comprising requesting a description of services offered by the device (Cho, Fig.17 discloses in steps 717 that the UPnP client, being on the external network, requests the description of services from the UPnP proxy server).

Regarding claim 19, the combination of Cho, IETF-Draft-SSDP, Buch and Ellison teaches the method of claim 18. Cho further teaches that the description of services is requested from the intermediary (Cho, Fig.17 discloses in steps 717 that the UPnP client requests the description of services from the UPnP proxy server, which is an intermediary).

Regarding claim 20, the combination of Cho, IETF-Draft-SSDP, Buch and Ellison teaches the method of claim 12.

Cho does not teach but Buch teaches receiving an approval authentication acknowledgement to the request; and responsive to the approval, requesting a service of the device (Buch, Figs. 7 and 8 discloses that the SIP caller receives a 200 OK as an approval authentication acknowledge to the SIP Request; and responsive to the 200 OK, the caller receives the service requested);

Examiner provides the same rationale as provided in claim 12 for the combination of Cho and Buch.

Regarding claim 22, the combination of Cho, IETF-Draft-SSDP, Buch and Ellison teaches the method of claim 12. Cho further teaches that a traveling control point performs the method for communicating with the device (Cho, Fig.1 discloses that a wireless internet client 110 communicates with the UPnP devices in a home network).

5. **Claims 13-14** are rejected under 35 U.S.C. 103(a) as being unpatentable over Cho, IETF-Draft-SSDP, Buch and Ellison as applied to claim 12 above, further in view of U.S. patent publication no. 2005/0111382 to Le et al. (hereinafter "**Le**").

Regarding claim 13, the combination of Cho, IETF-Draft-SSDP, Buch and Ellison teaches the method of claim 12.

Cho further teaches that the intermediary is configured to:

forward the request to the device (Fig.7 and [0026] disclose that the UPnP proxy server also includes a bridge for sending control messages to the UPnP devices in the home network);

monitor for an approval or disapproval authentication acknowledgement to the request (Fig.2, Fig.7 and [0026] disclose that the bridge receive event messages from the UPnP devices, where the event messages include responses to the previously sent control messages); and

Cho does not teach configuring a filter of the intermediary to allow communication with the device if an approval authentication acknowledgement is received.

However, in the same field of endeavor, Le discloses using firewall pinholes to dynamically filter network packets (see [0002]), where the firewall is an intermediary whose filtering rules are dynamically configured and applied based on the newly established or deleted network address bindings for authorized communications (see [0137] and [0138]).

It would have been obviousness for one of ordinary skill to combine Cho and Le so that a firewall is employed to allow communications between authenticated sessions only by using dynamically configured filtering rules. One would have been motivated to combine as such by Le's teaching of using an Internet firewall to secure an internal network from the Internet to the extent that it blocks unsolicited traffic from the outside.

Regarding claim 14, the combination of Cho, IETF-Draft-SSDP, Buch, Ellison and Le teaches the method of claim 13.

Cho does not teach but Le further teaches that the intermediary is further configured to configure the filter to block communication with the device is a disapproval authentication acknowledgement is received ([0054] disclose that a step of filtering further comprises blocking said data from being communicated through said filtering node onwards to the second terminal based on the binding, if such binding does not exist among the configured bindings).

Examiner provides the same rationale as provided in the rejection of claim 13 for the combination of Cho and Le.

6. **Claim 21 is** rejected under 35 U.S.C. 103(a) as being unpatentable over Cho, IETF-Draft-SSDP, Buch and Ellison as applied to claim 12 above, further in view of IETF RFC 3056, "Connection of IPv6 domains via IPv4 clouds", hereinafter "**RFC 3056**".

Regarding claim 21, the combination of Cho, IETF-Draft-SSDP, Buch and Ellison teaches the method of claim 12.

Cho does not teach but RFC 3056 teaches using the prefix of a globally unique IPv6 address to identify an intermediary that connects an IPv6 cloud to the IPv4 network.

It would have been obvious for one of ordinary skill to combine Cho and RFC 3056 so that the intermediary is identified by an IPv6 address prefix, which is a port of the IPv6 address. One would have been motivated to combine as such by Cho's disclosure of using IPv6 addresses on the internal network and IPv4 address on the external network.

7. **Claims 23, 25 and 26** are rejected under 35 U.S.C. 103(a) as being unpatentable over the U.S. patent application publication no. 2003/0217136 to Cho et al. (hereinafter "**Cho**"), in view of U.S. patent application publication no. 2003/0217165 to Buch (hereinafter "**Buch**"), and the article "UPnP™ Security Ceremonies Design Document For UPnP Device Architecture 1.0" authored by Ellison and published by the UPnP Forum (hereinafter "**Ellison**").

Regarding claim 23, Cho teaches a system of devices communicatively coupled with an internal network and an external network via a gateway (Cho, Fig. 1, UPnP Proxy server), comprising:

a first device, communicatively coupled to the internal network, offering services (Cho, Fig.1, UPnP devices); a second device selectively coupled with the internal and external networks,

the second device seeking a service of the first device (Cho, Fig.1, wired/wireless internet clients),

wherein when requesting the service, said requesting includes sending a communication initiation request to the first device to facilitate establishing a communication session with the first device; and an intermediary selectively communicatively coupling the first and second devices, wherein the intermediary is configured to receive a communication initiation request from the second device over the external network and forward the request to the first device (Cho, Fig. 1 discloses the wired/wireless internet clients sending control messages to the UPnP device via the UPnP Proxy server as an intermediary, which forwards messages to the UPnP device).

Cho does not disclose that the session to be established is a secure session.

However, in the same field of endeavor, Buch teaches a way of performing end-to-end user authentication to establish secure sessions using the SIP Invite request and responses, as disclosed in its Abstract.

It would have been obviousness for one of ordinary skill to combine Cho and Buch to have a system that establish secure sessions between two network terminal devices via by using end-to-end authentication. One would have been motivated to combine as such by Ellison's teaching of the need for a security model which need was recognized by the UPnP Forum at the time of the invention (see Ellison, page 3, section 1 “Background” and section 2 “Security Model”), and that Buch’s teaching of an end-to-end authentication mechanism provides a solution to the problem.

Regarding claim 25, the combination of Cho, Buch and Ellison teaches the system of claim 23. Cho further teaches that the first device communicates with the second device in accord with the UPnP Security Protocol (Cho, Fig. 1).

Regarding claim 26, the combination of Cho, Buch and Ellison teaches the system of claim 23. Cho does not teach but Ellison teaches that the secure communication initiation request corresponds to a UPnP Set Session Key (SSK) request (Ellison, page 13, section 5, "Session Keys").

It would have been obvious for one of ordinary skill in the art to combine Cho and Ellison so that the secure communication initiation request corresponds to a UPnP set session key request. One would have been motivated to combine Cho and Ellison by Ellison in that Ellison first discloses the need in UPnP for a security protocol and then suggested using Session Key to establish end-to-end secure sessions.

8. **Claim 24** is rejected under 35 U.S.C. 103(a) as being unpatentable over Cho, Buch and Ellison, as applied to claim 23 above, further in view of U.S. patent publication no. 2005/0111382 to Le et al., hereinafter "**Le**".

Regarding claim 24, the combination of Cho, Buch and Ellison teaches the system of claim 23. Cho does not teach but Buch teaches that the intermediary is further configured to monitor the first device for an approval or disapproval authentication acknowledgement for the request (Buch, Fig. 8 and [0051] discloses the SIP proxy as an intermediary that works between two SIP clients to forward SIP request and responses) .

Examiner provides the same rationale as provided in claim 23 for the combination of Cho and Buch.

Furthermore, Cho does not teach but Le teaches configuring a filter of the intermediary controlling communication (Le, [0002], [0137] and [0138] disclose that the firewall is an intermediary whose filtering rules are dynamically configured and applied based on the newly established or deleted network address bindings for authorized communications) over the first network from the first device based at least in part on a monitored authentication acknowledgement.

It would have been obviousness for one of ordinary skill to combine Cho and Le so that a firewall is employed to allow communications between authenticated sessions only by using dynamically configured filtering rules. One would have been motivated to combine as such by Le's teaching of using an Internet firewall to secure an internal network from the Internet to the extent that it blocks unsolicited traffic from the outside.

Allowable Subject Matter

9. **Claim 10** is objected to as being dependent upon the rejected base claim 1, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US 20040233904 A1, Saint-Hilaire, Ylian et al., Universal plug-and-play mirroring device, system and method;

US 20060143295 A1, Costa-Requena; Jose et al., System, method, mobile station and gateway for communicating with a universal plug and play network;

US 20030046703 A1, Knowles, Gregory T. et al., Systems and methods for facilitating user access to content stored on private networks;

US 20040249907 A1, Brubacher, Douglas Keith et al., Automatic discovery and configuration of external network devices;

US 20050149481 A1, Hesselink, Lambertus et al., Managed peer-to-peer applications, systems and methods for distributed data access and storage;

US 20050185658 A1, Kamiwada, Toru et al., Gateway apparatus connected to a plurality of networks forming respective different network segments, and program and method for transferring IP packets;

US 20070214356 A1, Song; Yu et al., Method and system for authentication between electronic devices with minimal user intervention;

US 20030126239 A1, Hwang, Hye-sook, Mobile communication terminal, network access system and method thereof using the same;

US 20050266826 A1, Vlad, Stirbu, Method for establishing a security association between a wireless access point and a wireless node in a UPnP environment;

US 20060215684 A1, Capone; Jeffrey M., Protocol and system for firewall and NAT traversal for TCP connections;

US 6779004 B1, Zintel; William Michael, Auto-configuring of peripheral on host/peripheral computing platform with peer networking-to-host/peripheral adapter for peer networking connectivity;

US 20040120344 A1, Sato, Naoyuki et al., Device discovery application interface;

US 20040133896 A1, Lym, Kevin K. et al., Network device application interface;

US 20060112417 A1, Son; Kyoung-ho et al., System and method for establishing secured connection between home network devices;

US 20060168656 A1, Stirbu; Vlad, UPnP VPN gateway configuration service;

US 20060156388 A1, Stirbu; Vlad et al., Method and apparatus for a security framework that enables identity and access control services;

US 20070143488 A1, Pantalone; Brett A., Virtual universal plug and play control point;

US 6098172 A, Coss; Michael John et al., Methods and apparatus for a computer network firewall with proxy reflection;

US 6154775 A, Coss; Michael John et al., Methods and apparatus for a computer network firewall with dynamic rule processing with the ability to dynamically alter the operations of rules;

US 6330562 B1, Boden; Edward B. et al., System and method for managing security objects;

US 7107612 B1, Xie; Ken et al., Method, apparatus and computer program product for a network firewall;

US 20050075842 A1, Ormazabal, Gaston S. et al., Methods and apparatus for testing dynamic network firewalls;

US 20020103898 A1, Moyer, Stanley L. et al., System and method for using session initiation protocol (SIP) to communicate with networked appliances;

US 20060168253 A1, Baba; Kensuke et al., Access control processing method;

US 20060168264 A1, Baba; Kensuke et al., Information processing device, information processing method, and computer program;

IETF RFC 3303, “MiddleBox Communication Architecture and Framework”, August, 2002;

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHIRLEY X. ZHANG whose telephone number is (571)270-5012. The examiner can normally be reached on Monday through Friday 7:30am - 5:00pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on (571) 272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. X. Z./
Examiner, Art Unit 4121

/Taghi T. Arani/
Supervisory Patent Examiner, Art Unit 4121
2/2/2008